IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

PATRICK PEROTTI, individually and on behalf of all others similarly situated, Plaintiff, v. CADWALADER, WICKERSHAM & TAFT LLP, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Patrick Perotti ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendant Cadwalader, Wickersham & Taft LLP ("Defendant") and alleges as follows:

JURISDICTION AND VENUE

1. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are members of the proposed Class who are diverse from Defendant, and (4) there are more than 100 proposed Class members.

2. This Court has general personal jurisdiction over Defendant because many of Defendant's partners are residents and citizens of this district, Defendant conducts substantial business in this district, and the events giving rise to Plaintiff's claims arise out of Defendant's contacts with this district.

3. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant is a resident and citizen of this district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this district.

PARTIES

4. Plaintiff Patrick Perotti is a resident and citizen of Ohio.

5. Defendant Cadwalader, Wickersham & Taft LLP is a New York limited liability partnership with its principal place of business in New York, New York.

FACTUAL ALLEGATIONS

I. Cadwalader, Wickersham & Taft LLP

6. Defendant is a New York-based, international law firm, and is one of the oldest, law firms in the United States.

7. Defendant employs over 400 attorneys and specializes in complex financial matters and transactions.

8. Defendant is or has been involved with numerous matters that require the collection and analysis of individuals' Personal Identifying Information ("PII"), such as shareholder derivative suits.

9. Defendant has an acute interest in maintaining the confidentiality of the PII entrusted to it and is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding PII in its possession.

10. To this point, Defendant's own website recognizes the importance of protecting PII from the substantial risks that exists: "Businesses today face constant, and constantly evolving, cybersecurity risk…Regulators, recognizing the threat posed by computer hackers to businesses and critical infrastructure, are constantly proposing and implementing new rules that require businesses to adopt comprehensive cybersecurity and data protection programs."

https://www.cadwalader.com/practice/business-fraud-white-collar-defense/cybersecurity-and-data-privacy.

II. The Data Breach

11. According to Defendant, on November 15-16, 2022, "an unauthorized third party gained remote access to its systems and acquired certain information from its network, including documents containing [] personal information."[1] (the "Data Breach").

12. The PII compromised in the Data Breach included individuals' name, Social Security number, and shareholding information.[2]

13. Defendant reports that it "took steps to stop the unauthorized access and began a thorough forensic investigation with the assistance of outside cybersecurity experts."[3]

14. Defendant does not state when it learned of the Data Breach or when it launched its investigation. However, more than four months passed from the date of the breach until Defendant issued notice to Plaintiff.

15. Approximately 93,211 individuals' PII was compromised in the Data Breach.

16. Defendant sent a letter to Plaintiff dated March 30, 2023, notifying them of the Data Breach. *See* Exhibit A.

17. Defendant's letter also offered free credit monitoring services to those potentially impacted by the Data Breach.

---

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/30f7a1de-50d4-4484-8eaa-1b01e624f123.shtml

[2] *Id.* Defendant's reference to "shareholding information" in its breach notice letter presumably refers to one or more shareholder derivate suits in which the affected individual is an absent class member. The unspecified "shareholding information" potentially includes financial accounts, account numbers, trading history, holdings, and balances.

[3] https://apps.web.maine.gov/online/aeviewer/ME/40/30f7a1de-50d4-4484-8eaa-1b01e624f123.shtml

18. Defendant did not state why it was unable to prevent the Data Breach or which security feature failed.

19. Defendant did not state why it did not contact individuals about the Data Breach until over four months after the Data Breach occurred.

20. Defendant failed to prevent the Data Breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

III. Injuries to Plaintiff and the Class

21. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiff's PII, Plaintiff and the Class have been damaged.

22. Plaintiff and the Class have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud. Plaintiff has spent approximately 11 hours monitoring accounts and taking other actions to protect his PII in response to receiving the breach notification letter.

23. In addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impacts caused by a breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[4]

24. In addition to fraudulent charges and damage to their credit, Plaintiff and the Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or

[4] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

25. Additionally, Plaintiff and the Class have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII is used, the diminution in the value or use of their PII, and the loss of privacy.

IV. The Value of PII

26. It is well known that PII, and social security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

27. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[5]

28. People place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[6]

29. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as

[5] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

[6] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

your DNA to hackers."[7] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[8]

V. Industry Standards for Data Security

30. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, Marriott, T-Mobile, and Capital One, Defendant is, or reasonably should have been, aware of the importance of safeguarding PII, as well as of the foreseeable consequences of its systems being breached.

31. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

[7] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

[8] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

i. Monitoring for server requests from Tor exit nodes.

32. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[9] and protection of PII[10] which includes basic security standards applicable to all types of businesses.

33. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

[9] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[10] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

34. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[11]

35. Because Defendant was entrusted with PII, it had, and has, a duty to keep the PII secure.

36. Plaintiff and the Class reasonably expect that when their PII is provided to a sophisticated business for a specific purpose, that business will safeguard their PII and use it only for that purpose.

37. Nonetheless, Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, it could have prevented the Data Breach.

CLASS ACTION ALLEGATIONS

38. Plaintiff, individually and on behalf of all others, brings this class action pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3), and (c)(4).

39. The proposed Class is defined as follows:

[11] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

Nationwide Class: All persons whose PII was maintained on Defendant's servers that were compromised in the Data Breach.

40. Plaintiff reserves the right to modify, change, or expand the definition of the proposed Class based upon discovery and further investigation.

41. *Numerosity*: The proposed Class is so numerous that joinder of all members is impracticable. Although the precise number is not yet known to Plaintiff, Defendant has reported that the number of persons affected by the Data Breach is 93,211.[12] The Class Members can be readily identified through Defendant's records.

42. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and obtaining their PII;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect PII as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and the Class's PII secure and prevent loss or misuse of that PII;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiff's and Class's PII;

h. Whether Defendant's conduct was intentional, willful, or negligent;

[12] https://apps.web.maine.gov/online/aeviewer/ME/40/30f7a1de-50d4-4484-8eaa-1b01e624f123.shtml

i. Whether the Class suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

j. Whether the Class is entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

43. *Typicality*: The claims of Plaintiff are typical of the claims of the Class. Class members were injured and suffered damages in substantially the same manner as Plaintiff, Class members have the same claims against Defendant relating to the same course of conduct, and Class members are entitled to relief under the same legal theories asserted by Plaintiff.

44. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the Class and has no interests antagonistic to those of the Class. Plaintiff have retained counsel experienced in the prosecution of complex class actions including, but not limited to, data breaches.

45. *Predominance*: Questions of law or fact common to Class members predominate over any questions affecting only individual members. Common questions such as whether Defendant owed a duty to Plaintiff and the Class and whether Defendant breached its duties predominate over individual questions such as measurement of economic damages.

46. *Superiority*: A class action is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of the Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendant's actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale, and comprehensive supervision over the entire controversy by a single judge in a single court.

47. *Manageability*: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

48. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

49. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

50. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

51. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

52. Defendant owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard their PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such

information and use it for nefarious purposes, but Defendant knew that it was more likely than not Plaintiff and Class members would be harmed by such exposure of their PII.

53. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

54. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

55. Defendant breached the aforementioned duties when it failed to use security practices that would protect the Plaintiff's and Class Members' PII, thus resulting in unauthorized third-party access to the Plaintiff's and Class members' PII.

56. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and Class members' PII within its possession, custody, and control.

57. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class members' PII was disseminated and made available to unauthorized third parties.

58. Defendant admitted that Plaintiff's and Class members' PII was wrongfully disclosed as a result of the Data Breach.

59. The Data Breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud or identity theft.

60. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care, including by: failing to adequately protect the PII; failing to conduct regular security audits; failing to timely identify the breach and notify Plaintiff and the Class; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII.

61. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised.

62. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class have been put at an increased risk of credit fraud or identity theft, and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiff and the Class for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of two years. Defendant is also liable to Plaintiff and the Class to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII. Defendant is liable to Plaintiff and the Class for the amount of time and efforts they have expended to protect themselves following the receipt of the breach notification letter. Defendant is also liable to Plaintiff and the Class to the extent their PII has been diminished in value because Plaintiff and the Class no longer control their PII and to whom it is disseminated.

COUNT II
UNJUST ENRICHMENT

63. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

64. Plaintiff and the Class have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Defendant and that was ultimately compromised in the Data Breach.

65. Defendant, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on security measures to secure Plaintiff's and the Class's PII.

66. Defendant also understood and appreciated that the PII pertaining to Plaintiff and the Class was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

67. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and the Class. Nevertheless, Defendant continued to obtain the benefits conferred on it by its possession of Plaintiff's and Class members' PII. The benefits conferred upon, received, and enjoyed by Defendant were not conferred gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

68. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff's and the Class's PII, Plaintiff and the Class suffered and continue to

suffer considerable injuries in the forms of, *inter alia,* attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, and increased risk of harm.

69. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiff and the Class, wherein it profited from interference with Plaintiff's and the Class's legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its conduct.

70. Accordingly, Plaintiff, on behalf of himself and the Class, respectfully requests that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically, the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff's and the Class's PII, and/or compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for a judgment against Defendant as follows:

a. For an order certifying the proposed Class, appointing Plaintiff as Representative of the proposed Class, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury.

Dated: April 12, 2023

Respectfully submitted,

/s/ Todd S. Garber

Todd S. Garber
Andrew C. White
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
1 North Broadway, Suite 900
White Plains, New York 10601
Tel: (914) 298-3281
Fax: (914) 908-6709
tgarber@fbfglaw.com
awhite@fbfglaw.com

Charles E. Schaffer (pro hac vice to be filed)
Nicholas J. Elia (pro hac vice to be filed)
LEVIN, SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215) 592-1500
cschaffer@lfsblaw.com
nelia@lfsblaw.com

Jeffrey S. Goldenberg (pro hac vice to be filed)
Todd B. Naylor (pro hac vice to be filed)
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Phone: (513) 345-8291
Facsimile: (513) 345-8294
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com

Counsel for Plaintiff and Proposed Class